INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG20-TD2207-R2

STUDY GROUP 20

Original: English

Question(s): 2/20 Virtual, 17-27 May 2021

TD

Source: Editors

Title: Output text of draft Supplement ITU-T Y.Sup-IoT-Eco-Plan "Framework for Internet of Things ecosystem Master Plan" - for agreement (Virtual, 17-27 May 2021)

Keywords: IoT ecosystem; Master Plan; Supplement; Technical Aspects

Abstract: This document contains the updated version of the draft Supplement ITU-T Y.Sup-IoT-Eco-Plan "Framework for Internet of Things ecosystem Master Plan" – for "agreement" at the May 2021 SG20 meeting.

This document contains the updated version of the new Supplement ITU-T Sup-IoT-Eco-Plan "Framework for Internet of Things ecosystem Master Plan", output of the Q2/20 meeting, Virtual, 17-27 May 2021 submitted for agreement to the May 2021 SG20 meeting.

The Supplement has been revised in the May 2021 Q2/20 meeting according to the meeting discussion results concerning contribution C876-R1 (global check of the document, including for definitions, acronyms, references, bibliography and clause 7.1.2), and other meeting agreements (these include – but are not limited to - additional editorial updates, such as those for consistency of upper/lower cases and acronyms).

Draft Supplement ITU-T Y.Sup.IoT-Eco-Plan

Framework for Internet of Things ecosystem Master Plan

Summary

A healthy Internet of Things (IoT) ecosystem can be an effective tool to increase industry competitiveness and citizens' wellbeing. There are many areas where IoT can be deployed, such as agriculture, health care, consumer goods, industry, and education, and it may not be practical or possible to act on all verticals at the same time. An IoT Master Plan is intended to focus resources on priority verticals or areas with the aim of producing more effective results taking into consideration the country's particular environment (e.g., challenges and opportunities) and priorities.

When defining this Master Plan, it is important to consider international benchmarking and have a holistic methodology that considers the country's priorities but also takes into account the potential demand, supply and development capacity when selecting priority vertical domains. It's also crucial to engage relevant stakeholders, including those from various verticals, industries, government, academia and civil society throughout the process, from plan development to execution, to support effective deployment.

Therefore, this Supplement describes a framework to support Member States to define their IoT ecosystem Master Plan, based on vertical domain assessment and identification of technical aspects to support the selected verticals. It also presents some actions to support the Master Plan deployment.

Keywords

IoT ecosystem, Master Plan, technical aspects.

CONTENTS

List of Tables

List of Figures

Draft Supplement ITU-T Y.Sup-IoT-Eco-Plan

Framework for Internet of Things ecosystem Master Plan

1 Scope

This Supplement describes a framework to support Member States to define their Internet of Things (IoT) ecosystem Master Plan, based on vertical domain assessment and technical aspects for the selected verticals. It also presents some actions to support the Master Plan deployment.
Therefore, this document covers the following items:

– Technical aspects when defining the IoT ecosystem Master Plan;
– Vertical domain assessment;
– Actions to support the Master Plan deployment.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this document are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

ITU-T L.1400 Recommendation ITU-T L.1400 (2011), *Overview and general principles of methodologies for assessing the environmental impact of information and communication technologies*

ITU-T X.1252 Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*

ITU-T Y.101 Recommendation ITU-T- Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*

ITU-T Y.4000 Recommendation ITU-T Y.4000 (2012), *Overview of the Internet of things.*

ITU-T Y.4050 Recommendation ITU-T Y.4050 (2016), *Terms and definitions for the Internet of things*

ITU-T Y.Sup.53 Supplement ITU-T Y.Sup.53 to ITU-T 4000 Series, (2019), *IoT Use Cases*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.2 interoperability [ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged**.**

3.1.3 thing [ITU-T Y.4000]: In the Internet of things, object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

API	Application Programming Interface
ATM	Automated Teller Machine
ICT	Information and Communication Technology
IoT	Internet of things
POS	Point of Sale
RAN	Radio Access Network
R&D	Research and Development
SDO	Standards Developing Organization

5 Introduction

The Internet of things (IoT) is a global infrastructure for the information society which provides opportunities to increase the efficiency of systems and processes, enable new services and improve people's quality of life.

IoT is considered as the technological solution capable of impacting not only the productive chain of Information and Communication Technology (ICT), but something capable of causing a true digital revolution [b-INDUST].

This Supplement aims to define a framework to assist Member States in prioritizing verticals for the development of the IoT ecosystem.

The IoT ecosystem is usually quite large and a prioritization of verticals is expected in order to increase economic and technological growth.

This Supplement focuses on how administrations can identify their strategic needs to guide the prioritization of verticals, analyze technical aspects that support the expansion process of the IoT ecosystem, and to ensure greater efficiency in the results of the IoT ecosystem Master Plan.

A model of the Action Plan structure is also presented.

6 Strategic positioning

The strategic positioning will enable the country to define its strategy of action, define its critical success factors and prioritize them. In terms of IoT ecosystem, the definition of the strategic positioning represents an important step towards directing the country's efforts and mobilizing the main actors to reach relevant objectives. Objectives and priorities may be related to different aspects of the IoT ecosystem, for instance IoT adoption as well as IoT manufacturing or innovation.

Moreover, the strategic positioning should be contained in a country’s expectation, which can be achieved by analyzing two aspects: what are the country's main objectives in relation to IoT and the number of priority verticals that the country intends to focus on [b-ASPIRA].

The positioning of countries in relation to the two aspects allows them to be grouped into four groups:

■ Group 1: countries seeking global leadership in IoT, both in the development and implementation of IoT.

■ Group 2: countries seeking leadership in specific verticals. This is adopted by countries that have chosen to develop distinctively a limited number of verticals.

■ Group 3: countries seeking usage of IoT to increase competitiveness and generate well-being for the population. These countries are focused on the development of IoT as a lever to increase the competitiveness of the local industry, generate jobs and improve the quality of life of the population.
■ Group 4: countries aiming to improve the quality of life via the support of IoT. They are focused on the development of IoT in smart cities, with the aim of improving the quality of life of the population.
In addition, defining the government's role and its degree of involvement in IoT ecosystem formation, and building robust governance that ensures broad stakeholder participation from the outset, are also important steps in the process.

7. Technical aspects when defining the IoT ecosystem Master Plan

The elaboration of the IoT ecosystem Master Plan must consider some technical aspects that influence the Master Plan and subsequent paths to be followed to achieve the objectives.
In this sense, the challenges presented in this clause are important for a country to formulate the IoT ecosystem Master Plan [b-REPORT].

7.1 Connectivity

The connectivity aspect is a primary element in expanding the IoT ecosystem. The connectivity aspect is described below in detail from the perspectives of infrastructure, spectrum and devices.

7.1.1. Infrastructure

It is assumed that for the technology's expansion and business models involving IoT communications to take place, some level of infrastructure needs to be in place to provide the coverage and connectivity necessary to enable IoT applications. The variety of environments and connectivity technologies used by IoT solutions also needs to be taken into consideration.
One of the important infrastructure-related steps is an assessment of the country's telecommunications infrastructure, such as data transport and access networks, and identifying structural strengths and/or lacks that may impact IoT applications.
That assessment should guide the elaboration of projects aimed at addressing the identified deficiencies: for example, expansion of networks, such as high-capacity fiber-optic networks, radio-frequency data transport network, and mobile data networks, including for remote locations not yet covered.
In this sense, maintaining a regularly updated register on existing and developing telecommunications networks in the country would support efficient allocation of resources..
When deploying IoT solutions in numerous verticals domains, such as logistics, public transport, traffic management, electricity, smart vehicles, water abstraction, among others, it is necessary for the infrastructure to support different IoT environments composed with devices, sensors and user terminals with distinct requirements, that will be interconnected to provide intelligent solutions for citizens, businesses and public sector. Therefore, it is essential that the Master Plan takes into consideration relevant infrastructure expansion, including coverage, connectivity, capacity, and high device connection density, that will support these heterogeneous IoT environments. For example, the Master Plan could focus on fiber deployment and/or wireless connectivity such as 5G.
It can be complex and costly to expand the infrastructure, so the Master Plan should incentivize efficient use of the already deployed infrastructure elements, for example by using tools such as sharing of passive infrastructures (e.g., poles, ducts and towers), Radio Access Network (RAN) and optical fiber Sharing.
For instance, given that more mature segments such as electricity and telecommunications already have legacy infrastructure with relevant capillarity, infrastructure sharing appears as an option for the economic and efficient use of these inputs, reducing fixed costs in a model of distribution offer.

7.1.2. Spectrum

Spectrum use is one of the key aspects that should be considered when defining the Master Plan to develop the IoT ecosystem. Although there is no specific frequency band allocation for IoT applications, the Master Plan should take into account aspects like:

a) the potential benefits that can be clearly achieved by harmonized spectrum use that enables cost-effective and time-efficient deployment of IoT ecosystems;

b) the impact of harmful interference caused by radio frequency on some applications that require greater reliability and availability;

c) the necessity for more spectrum for IoT applications, which may be obtained by expanding the number of available spectrum frequencies for licensed mobile service and also for unlicensed bands.

d) the impact of the deployment of large networks in unlicensed bands on other applications that use the same frequency band.

Assessment of a country's unique environment will help to determine if it is appropriate or useful to identify frequency ranges for particular IoT applications. Identifying frequency ranges for a particular IoT application needs to take into consideration several aspects that naturally involve the licensed or unlicensed use of the above ranges, according to their intended purpose: for example, equipment price, market time, network coverage, reliability and resilience.

7.1.3. Devices

With the increasing adoption of IoT solutions across sectors, the world is experiencing a raise in IoT devices capable of radio frequency communication [b-CISCO-Forecast].

This massive increase of IoT devices can bring some risks to the network if devices do not adequately adopt IoT best practices or internationally recognized technical standards. Therefore, the Master Plan should take into consideration and may encourage conformance assessment to assure that these technical standards are implemented by the IoT devices manufactures.

Conformance assessment should be flexible and efficient (e.g., self-assessment) in order to not impose unnecessary delays to the deployment of new IoT devices and solutions that are crucial for the digital transformation.

7.2 Interoperability

IoT devices are quite heterogeneous, and therefore have different connectivity requirements, for example in terms of bandwidth, communication range, power consumption and hardware cost. To address this variety of requirements, several wireless communication protocol stacks have been defined and implemented. Similarly, there are also several protocol standards at the application layer. Providing interoperability between these various protocols is one of the major IoT challenges.

Interoperability in IoT can be classified as device interoperability, networking interoperability, syntactic interoperability, semantic interoperability, and platform interoperability, as shown in Figure 1 [b-INTEROP].

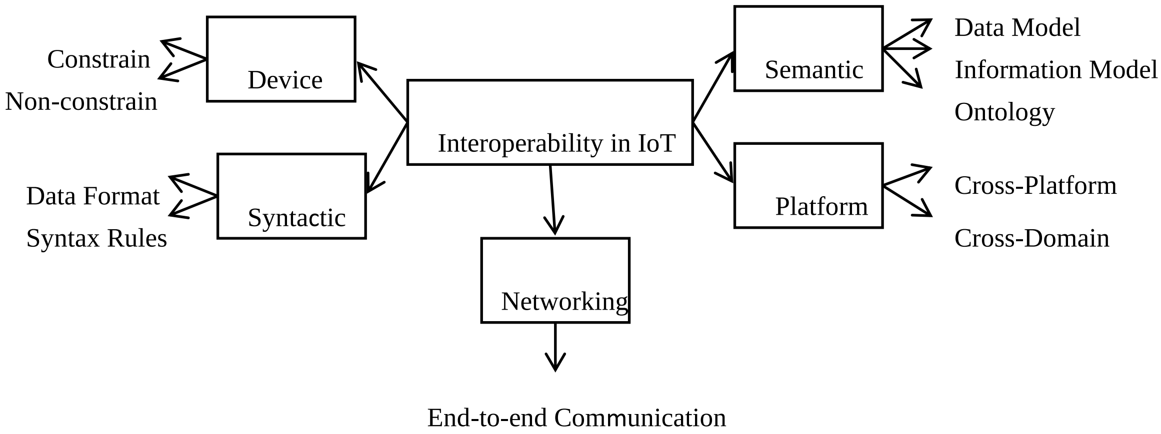

Figure 1 – IoT interoperability taxonomy

7.2.1 Device Interoperability

IoT devices are classified as non-constrained and constrained devices. The non-constrained devices have no limitation in terms of resources and computational capabilities, while the constrained devices are limited in terms of energy, processing power and communication capabilities. Those different characteristics contribute to the development of several communication protocols [b-INTEROP].

Therefore, the interoperability is crucial for device communication. In this way, device interoperability can be considered as the integration and interoperability of such heterogenous devices with various communication protocols at the device level.

7.2.2 Network Interoperability

Network interoperability provides messages exchange between different networks for end-to-end communication. Considering that IoT generally relies on various networks that may be intermittent and unreliable, network interoperability should handle issues such as addressing, routing, resource optimization, security, and mobility support.

7.2.3 Syntactical Interoperability

Syntactical interoperability refers to the data format interoperation used to exchange information between heterogeneous IoT systems. Each IoT resource defines its interfaces composed of messages sent sequentially with its own format using syntax rules. The communication between the source and the destination can be established when these syntax rules are compatible.

7.2.4 Semantic Interoperability

Data model, ontology and information model enable semantics, e.g., how data and metadata are exposed through Application Programming Interface (API)). In IoT, semantic interoperability enables automatic machine-to-machine communication.

7.2.5 Platform Interoperability

Platform interoperability adapts applications from one platform to another through their specific APIs and information models. There are two types of platform interoperability: cross-platform interoperability and cross-domain interoperability. The cross-platform interoperability enables interoperability across separate IoT platforms related with one vertical domain such as smart home, smart healthcare, smart garden, etc. As an evolution, the cross-domain interoperability enables interoperability between different platforms within different vertical domains.

7.3 Data Privacy and Security

Best practices and standards should be taken into account at every stage of the IoT ecosystem Master Plan development and implementation to adopt appropriate safeguards.. Other relevant national strategies, such as a national cyber security strategy, should also be taken into account in the development of an IoT ecosystem Master Plan. A user-centric approach should be taken to any consideration of security, best practices, and safeguards. Safeguards include assessment frameworks such as risk assessments and data protection and privacy impact assessments. Devices have varied capabilities, which may impact their ability to support security best practices and need to be taken into account. The information security and the security of the IoT ecosystem as a whole should be considered when developing and implementing a Master Plan.

Broad stakeholder consultation on these and related issues should be adopted and encouraged early in the Master Plan development process, including the initial design phase, and continue through implementation. Key stakeholders may include industry, internationally recognized Standards Developing Organizations (SDOs), civil society organizations, and individuals. Privacy policies as defined in [ITU-T X.1252] should be developed and adopted where possible to protect the information and rights of individuals.

8. Verticals domains assessment

Prioritizing verticals for applying or developing IoT solutions is a relevant step in the process of building a policy for IoT that aims to drive efforts and capture the greatest possible benefit [b-REPORT]. Therefore, is it important to prioritize:

- Direct efforts of government, private sector and academia;
- Optimize time and resources for environments where government action is integral;
- Capture the greatest possible benefit of IoT considering the available resources.

8.1 Verticals

The delimitation between verticals is based on the use cases, which represent the basic cell for calculating the impact that IoT can achieve and is based on the benefits that IoT can provide.

In general, use cases can be grouped by different factors such as sectors or environments. Sectors are known as traditional “economic segments”. This segmentation is relevant because it is a familiar way to look at companies within the same sector that may have operational similarities, such as mining, automotive, retail and agriculture.

However, some important IoT features are transversal to more than one sector. For this reason, grouping by environments is a better choice. This type of grouping is done by specific use cases composition that generates IoT value. Usually, the names used to group these IoT use cases, as application environments, should be simple and direct, which facilitates understanding, like cities, houses, shops, vehicles and factories. Among the reasons for the classification by application environments, the followings can be mentioned:

1) Representation more aligned with the user vision. For example, a family, that owns a house with automated daily tasks, can understand better the application environment “house” instead of the sectors “consumer goods” and “electronics” which compose the solution.

2) The need of interoperability. The application environments need interoperability among each other to increase the IoT benefits for the users.

3) Application environments classification as the reference structure for some public and private sectors.

The application environments identification, and consequently the vertical domains, vary according to the specificity of each country - different IoT vertical examples are shown in [ITU-T Y.Sup.53]. In order to identify the vertical domains, a large participatory process is necessary, including, not limited to, involvement of forums, different stakeholders (e.g., government, academia, companies, advisers, specialists and members of study committees), contributions through public consultations and IoT related workshops.

Table 1 provides an example of vertical domains grouped by application environments that a country has used in its prioritization process [b-REPORT].

NOTE - For the creation of this table, the applications identified in [ITU-T Y.Sup.53] have been grouped in the selected application environments.

Table 1 – Example of application environments used for prioritization

Application environments	Description	Applications
Vehicles	Vehicles, including cars, trucks, ships, airplanes and trains.	Vehicle tracking, e-call, V2X applications, traffic control, navigation, infotainment and fleet management
Health Care	Monitor and maintain human well-being and health.	Remote monitoring of patient after surgery (e-health), remote diagnostics, medication reminders, tele-medicine and wearable health devices
Store	Environments with high interaction with consumers, such as fairs, shows, cultural spaces, markets, hotels, concert halls, restaurants and banks.	Kiosk, Vending machines, retail stores, retail management, Point of sale (POS), Automated Teller Machine (ATM), digital signage and handheld terminals and customer feedback
Cities	Urban environments and utilities.	Intelligent transport System, waste management, street light control system, water distribution, smart parking, smart metering, smart grid, electric line monitoring, gas / oil / water pipeline monitoring, safety, commercial and home monitoring, surveillance camera applications, video analytics and sending alerts and fire alarm
Building	Smart homes, public and private smart offices.	Home alarm systems, connected appliances, smart lighting system and home entertainment
Rural	Rural environments with standardized production for agricultural or livestock culture.	Remotely controlled irrigation pump, crop management, soil analysis and livestock monitoring
Industry	Factories and production environments.	Proactive maintenance of machines, shop floor monitoring and industry automation
Logistic	Logistics chain outside urban environments, considering railways, air, river and land.	Asset tracking and remote container tracking naval

8.2 Vertical prioritization process

The prioritization process can be structured in three stages [b-REPORT]:

- Establishment of criteria and metrics: after analyzing several frameworks and methodologies for prioritizing verticals, twenty criteria are suggested, divided into three main axes: demand, supply and development capacity**.** It is clear that each country, based on its particularities, may suggest new criteria according to its needs;
- Definition of weights: in this stage the engaged stakeholders define the relative importance of the criteria, so that they are aligned with the expectation of the country in IoT;
- Vertical evaluation: all verticals are analyzed according to the defined criteria, assigning notes for each criterion that is weighted with the weights defined in the previous step.

8.3 Prioritization criteria tree

The prioritization process should be designed in a way to capture the particularities of the IoT context analysed. As mentioned before, three attributes have been defined that serve as pillars. The first pillar, demand, and shows the country's demand for IoT solutions in a given application environment. This demand can be measured in the form of challenges and opportunities to be addressed by the IoT. The second pillar, supply, measures the country's ability to offer IoT solutions for a specific application environment. These solutions can be measured by the local skills and opportunities of the country's ICT industry. And finally, the third pillar, development capacity, represents a combination of the efficiency of institutions, enabling elements, stakeholder capacity and government mobilization capacity.

Each attribute is divided into sub-attributes based on economic, social, productive and capacity aspects. The attributes/sub-attributes classification serves as the basis for the initial criteria tree building.

On the other hand, the criteria are selected considering their relevance to the project, their ability to differentiate application environments and the existence of related metrics. Some criteria have quantitative metrics applicable to the verticals and can be calculated from indicators while the members of the engagement forums [b-REPORT] must evaluate other criteria in a qualitative way.

Table 2 provides an example of prioritization criteria tree used by a country in order to prioritize the verticals in its Master Plan [b-REPORT]. The weights assigned to each sub-attribute and the notes obtained by criteria are shown (considering equal weights to the criteria pertaining to each sub-attribute).

Table 2 - Example of prioritization criteria tree

Attribute	**Sub-attribute**	**Sub-attribute Weight**	**Criteria**	**Notes**		
				Minimum	Maximal	Average
Demand	economic impact / competitiveness	50%	economic impact of IoT	30%	50%	38%
			increased productivity	35%	43%	38%
			increase in the production of goods with higher added value	15%	32%	24%
	socio-environmental impact	50%	impact on employment and income	23%	40%	34%
			improvement in quality of life	35%	56%	42%

			reduction of environmental impact	20%	31%	24%
Supply	strengthening the supply chain of IoT (supply)	100%	IoT companies	27%	52%	44%
			potential of insertion into the global productive chain of IoT	13%	37%	29%
			availability of private capital for innovation	20%	37%	28%
Development capacity	efficiency of institutions	50%	competitiveness in the IoT application environment	28%	39%	33%
			governance structure that allows coordination between the actors	31%	40%	37%
			ease of developing innovation and business environment	27%	35%	31%
	enabling elements	30%	tools for investment, financing and development	10%	24%	16%
			internationalization capacity	7%	17%	12%
			connectivity infrastructure	18%	40%	27%
			regulatory aspects related to IoT applications	14%	25%	20%
			security	9%	15%	12%
			data	9%	15%	12%
	mobilization capacity	20%	capacity of the government to encourage (supply)	45%	57%	50%
			capacity of the government to encourage (demand)	43%	55%	50%

9. Framework for support of the Master Plan implementation

The guiding principles of the Master Plan should be defined taking into consideration the strategic chosen to develop the IoT ecosystem. Based on the country’s expectation, vision of each vertical could be established, unfolded into strategic goals that identify the vertical challenges to be solved by IoT in order to deliver value to the society.

A Master Plan could be organized in four layers for each vertical: vision , strategic goals, specific goals and initiatives, that are unfolding from each other, and allow to understand the Action Plan and how it will be achieved [b-ACTION]. Figure 2 outlines the structure of the Action Plan [b-REPORT], in which the top achievement depends on the lower layers. Once the initiatives are being completed, the specific goals, the strategic goals and, ultimately, the vision will be reached.

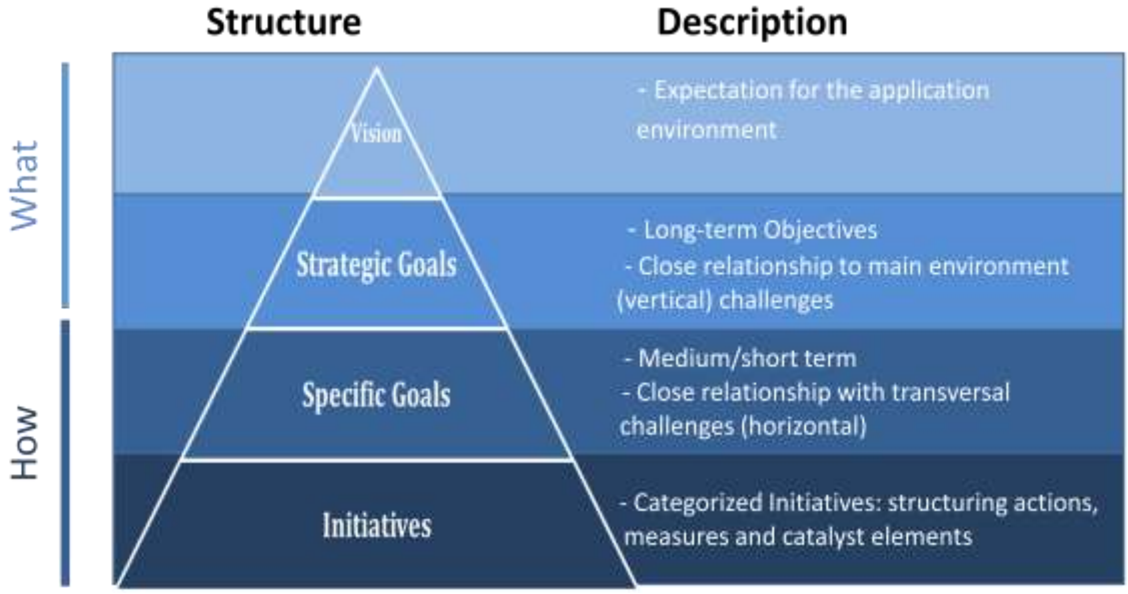

Figure 2. Structure of the Action Plan

The Action Plan is guided by "what" and "how" questions. The "what" question begins with a vision that expresses the long-term expectation related with IoT for the country [b-ASPIRA]. This vision is also called "environment vision" since it is defined for each vertical previously prioritized.
The next step is to unfold the strategic goals, which identify the environmental challenges that IoT needs to solve, in order to deliver value to the society. The strategic goals show the way to reach the vision for each vertical. Together with the vision, strategic goals are considered long-term goals.
Then, by the "how" questions, the strategic goals are broken down into specific goals. While the strategic goals work with verticals, the specific goals work with the horizontals and their realization can be considered medium/short term. The specific goals identify the way to achieve the strategic goals. Horizontal examples defined by a country are shown in table 3 [b-ACTION]:

Table 3 – Example of Action Plan

Horizontal efforts	Specifics goals
International Innovation	Encourage experimentation, cooperation and dissemination of successful business models; Improve and disseminate financial instruments for ICTs and innovative companies; Build environment for continuous monitoring of the Master Plan; Internationalize local solutions aligned with global standards.
Human Capital	Promote IoT qualified workforce; Raise youth interest in IoT/ICT; Improve Research and Development (R&D)and IoT engineering; Promote IoT training for public managers.
Regulatory, Security and Privacy	Discuss telecommunications regulatory issues in order to accelerate IoT applications development;

	Promote an adequate regulatory framework for personal data protection to foster innovation and individual rights protection; Identify specific regulatory issues related with the prioritized verticals; Establish an institutional design to face the privacy and security challenges of IoT.
Connectivity and interoperability infrastructure	Expand the telecommunication networks in accordance with the IoT services demands; Work with public policies to increase infrastructure for connectivity; Promote interoperability and network standardization related with networks, devices and IoT solutions.

Finally, each specific objective brings initiatives, which represent a set of actions, with one or more actors. Therefore, initiatives make tangible the specific goals focus on actions with clarity on the actors involved. The creation of initiatives needs prioritization that is based on three main criteria: ecosystem impact, implantation facility and alignment with the country's expectation. From there, it is possible to categorize the initiatives into three types, as shown in table 4 [b-ACTION]: structuring actions, measures and catalyst elements.

Table 4 – Example of initiative types

Initiative type	Decision makers	Impact	Deployment
Structuring actions	Decisions made by high-level engaged public entities.	High but limited to IoT development.	Challenging but possible if public entities are aligned.
Measures	Decisions made by management level of engaged entities.	Medium but limited to IoT development.	Medium and often already underway.
Catalyst elements	Decisions taken by high level forums, such as presidency and congress.	Very high and not limited to IoT development.	Very challenging and in general long-term resolution.

The structuring actions are fundamental and have high priority. Leaders are responsible for the Action Plan development. The measures complement the structuring actions, they are important but not strictly necessary for the IoT development, although they have great catalytic power. Once implemented, they increase the IoT impact in terms of economy and competitiveness. The measures progress needs to be monitored by the Master Plan, but with less intensity than structuring actions. Finally, the catalyst elements are initiatives that go beyond the IoT or even require other government discussion matters, like taxation. Such elements are understood as capable of enhancing the IoT effect.

As identified earlier, engagement by relevant stakeholders throughout the process of Master Plan development and execution is vital. Stakeholders such as government, industry, academia, and civil society have valuable expertise, interest, and role to play in different elements of the IoT ecosystem. Engagement by stakeholders can be facilitated in a number of manners. For example, when developing the Master Plan, the government could coordinate a multistakeholder coordination group to help identify the vision, strategic goals, and develop practical initiatives. When deploying the plan, different stakeholders may join together to form consortiums or action groups to deliver on specific goals or initiatives in the Master Plan. Government may also facilitate multistakeholder initiatives and support the work of Small and Mid-size Enterprises (SMEs)and/or innovators through calls for joint proposals or grants related to the strategic aims of the Master Plan. Likewise, current policy or regulatory environments may need to be reviewed in order to facilitate or encourage investment in the IoT ecosystem by industry or other stakeholders.

Bibliography

[b-BENCHMARK]	Product 1 - Benchmark of public policies and initiatives https://www.bndes.gov.br/wps/wcm/connect/site/48fff464-7a3c-442b-98c3-aa4634ad08d8/Relatorio-de-benchmark-fase-1-20170516_Produto_Frente_1_Benchmark_ENTREGA_FORMAL_FinalRevisado.pdf?MOD=AJPERES&CVID=lNGCXmw
[b-ROADMAP]	Product 2 - Technological Roadmap https://www.bndes.gov.br/wps/wcm/connect/site/1970e8af-33d4-48a5-9522-d6335c931e26/170614_Produto_Parcial_Frente+2_Sumario_Executivo_Roadmap_Final.pdf?MOD=AJPERES&CVID=lOOitOz
[b-REPORT]	Product 9 - Final Report of the IoT National Plan Study https://www.bndes.gov.br/wps/wcm/connect/site/d22e7598-55f5-4ed5-b9e5-543d1e5c6dec/produto-9A-relatorio-final-estudo-de-iot.pdf?MOD=AJPERES&CVID=m5WVIld
[b-INDUST]	The Fourth Industrial Revolution (2017), Klaus Schwab.
[b-PRIORITY]	Product 6 – Vertical and Horizontal Priorization Report https://www.bndes.gov.br/wps/wcm/connect/site/9cc660de-bb54-408a-a7e9-322f5dbc3f03/Produto+6_Relat%C3%B3rio_Final_Prioriza%C3%A7%C3%A3o_v1_atualizado.pdf?MOD=AJPERES&CVID=m0SUIir
[b-ASPIRA]	Product 3 – Supply and Demand Analysis – Expectation Report from Brazil to IoT https://www.bndes.gov.br/wps/wcm/connect/site/d1348f10-c93d-408e-8c2d-a2c2a6e4efb1/170614_Produto_Parcial_Frente+3_Aspiracao_IoT_Final.pdf?MOD=AJPERES&CVID=lOOiRj1
[b-ACTION]	Product 8 - Action Plan Report https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok

[b-CISCO-Forecast] Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256794

[b-INTEROP] Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Netw Appl 24, 796–809 (2019) Noura, M., Atiquzzaman, M. & Gaedke, M.